Allocation of Information Security Requirements to Security Enclaves Based on System Risk and Criticality –Low Risk

Low Risk Protection Profile Requirement	WAN	LAN/ Facility Comm.	Application System
3.8.5.A All NAS systems shall provide the required level of **security functionality and security integrity** based upon vulnerability, threat, and risk analyses. The threat analysis, risk analysis, and risk mitigation priority are documented in Section 3 of a Protection Profile and Security Target. This information is used to determine the security objectives stated in Section 4 and the security functional requirements, security assurance requirements, and evaluation assurance level specified in Section 5.	X		
3.8.5.B All NAS systems shall provide the required level of **security training** based upon the vulnerability, threat, and risk analyses.			
ADO_DEL.1 Delivery procedures	X	X	X
ADO_IGS.1 Installation, generation, and start-up procedures	X	X	X
AGD_ADM.1 Administrator guidance	X	X	X
AGD_USR.1 User guidance			X
3.8.5.C All NAS systems shall be protected from threats to compromise **integrity**.			
FDP_DAU.1 Basic data authentication	X	X	X
FDP_ROL.1 Basic rollback			X
FDP.SDI.1 Stored data integrity monitoring			X
FDP_UIT.1 Data exchange integrity	X	X	
FPT_AMT.1 Abstract machine testing	X	X	X
FPT_FLS.1 Failure with preservation of secure state	X	X	X
FPT_ITI.1 Inter-TSF detection of modification	X	X	

Low Risk Protection Profile Requirement	**WAN**	**LAN/ Facility Comm.**	**Application System**
FPT_ITT.1 Basic internal TSF data transfer protection	X	X	X
FPT_PHP.2 Notification of physical attack	X	X	X
FPT_PHP.3 Resistance to physical attack	X	X	X
FPT_RPL.1 Replay detection	X	X	X
FPT_TDC.1 Inter-TSF data consistency			X
FPT_TRC.1 Internal TSF consistency			X
FPT_TST.1 TSF testing	X	X	X
3.8.5.D All NAS systems shall be protected from threats to compromise **availability**.			
FPT_ITA.1 Inter-TSF availability	X	X	
FRU_FLT.1 Degraded fault tolerance	X	X	X
FRU_PRS.1 Limited priority of service	X	X	X
FRU_RSA.1 Maximum quotas	X	X	X
3.8.5.E All NAS systems shall provide **access control**.			
FDP_ACC.2 Complete access control	X	X	X
FDP_ACF.1 Security attribute based access control	X	X	X
FDP_ETC.1 Export of user data without security attributes	X	X	X
FDP_IFC.1 Subset information flow control	X	X	X
FDP_IFF.1 Simple security attributes	X	X	X
FDP_IFF.5	X	X	X

Low Risk Protection Profile Requirement	WAN	LAN/ Facility Comm.	Application System
No illicit information flows			
FDP_ITC.1 Import of user data without security attributes	X	X	X
FPT_SEP.1 TSF domain separation	X	X	X
3.8.5.F All NAS systems shall provide an **audit** capability sufficient to monitor attempted and successful system intrusions.			
FAU_ARP.1 Security Alarms	X	X	X
FAU_GEN.1 Audit data generation	X	X	X
FAU_GEN.2 User identity association	X	X	X
FAU_SAA.2 Profile based anomaly detection	X	X	X
FAU_SAA.4 Complex attack heuristics	X	X	X
FAU_SAR.1 Audit review	X	X	X
FAU_SAR.2 Restricted audit review	X	X	X
FAU_SAR.3 Selectable audit review	X	X	X
FAU_SEL.1 Selective audit	X	X	X
FAU_STG.2 Guarantees of audit data availability	X	X	X
FAU_STG.4 Prevention of audit data loss	X	X	X
FPT_STM.1 Reliable time stamps	X	X	X
3.8.5.G All NAS systems shall provide for information **confidentiality** based upon the result of a security assessment.			
FDP_RIP.2 Full residual information protection			X
FDP_UCT.1	X	X	

Low Risk Protection Profile Requirement	**WAN**	**LAN/ Facility Comm.**	**Application System**
Basic data exchange confidentiality			
FPR_ANO.1 Anonymity	X	X	X
FPT_ITC.1 Inter-TSF confidentiality during transmission	X	X	
FPT_ITT.1 Basic TSF data transfer protection	X	X	
3.8.5.H NAS systems shall implement **identification and authentication** at a level based upon a security assessment, and non-repudiation when appropriate.			
FIA_AFL.1 Authentication failure handling	X	X	X
FIA_ATD.1 User attribute definition	X	X	X
FIA_SOS.1 Verification of secrets	X	X	X
FIA_SOS.2 Generation of secrets	X	X	X
FIA_UAU.2 User authentication before any action	X	X	X
FIA_UAU.3 Unforgeable authentication	X	X	X
FIA_UAU.6 Re-authenticating	X	X	X
FIA_UAU.7 Protected authentication feedback	X	X	X
FIA_UID.2 User identification before any action	X	X	X
FIA_USB.1 User-subject binding		X	X
3.8.5.I All NAS systems shall provide **recovery** measures from security incidents.			
FDP_UIT.3 Destination data exchange recovery	X	X	X
FPT_RCV.3 Automated recovery without undue loss	X	X	X

Low Risk Protection Profile Requirement	WAN	LAN/ Facility Comm.	Application System
FPT_RCV.4 Function recovery	X	X	X
3.8.5.J All NAS systems shall provide the capability to centrally **manage** security functions.			
FMT_MOF.1 Management of security functions behavior	X	X	X
FMT_MSA.1 Management of security attributes	X	X	X
FMT_MSA.2 Secure security attributes	X	X	X
FMT_MSA.3 Static attribute initialization	X	X	X
FMT_MTD.1 Management of TSF data	X	X	X
FMT_MTD.2 Management of limits on TSF data	X	X	X
FMT_MTD.3 Secure TSF data	X	X	X
FMT_REV.1 Revocation	X	X	X
FMT_SAE.1 Time-limited authorization	X	X	X
FMT_SMR.1 Security roles	X	X	X
FTA_LSA.1 Limitation on scope of selectable attributes			X
FTA_MCS.1 Basic limitation on multiple concurrent sessions			X
FTA_SSL.1 TSF-initiated session locking			X
FTA_SSL.3 TSF-initiated termination			X
FTA_TAB.1 Default TOE access banners			X
FTA_TSE.1 TOE session establishment			X